AO 106 (Rev. 04/10) Application for a Search Warrant

EC

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the Twitter profile for the usernames @JIMMY43845156 and @ ALWAYSHORNY695 that is stored at premises controlled by Twitter.

Case No. 2:21-mj-551

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Secs 2252 and 2252A	Receipt/possession/accessing with intent to view of child pornography/visual depictions of minors engaged in sexually explicit conduct in interstate commerce

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew McCabe, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: August 23, 2021

City and state: Columbus, Ohio

Kimberly A. Johnson
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:	)	
	)	
Information associated with the Twitter profile	)	Case No. 2:21-mj-551
for the Username: @JIMMY43845156 at	)	
https://twitter.com/JIMMY43845156; and	)	Magistrate Judge
the Twitter profile for @ ALWAYSHORNY695	)	
at https://twitter.com/ALWAYSHORNY695	)	
that is stored at premises controlled by Twitter.	)	**Filed Under Seal**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrew D. McCabe, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent with the FBI assigned to the Cincinnati Division, Cambridge Resident Agency and I have been a Special Agent since September 2010. I am currently assigned to Cambridge Resident Agency and I am a member of the Child Exploitation and Human Trafficking Task Force. During my tenure as an FBI Special Agent, I have investigated numerous crimes including, but not limited to, bank robbery, drug trafficking, racketeering, kidnaping, violent extremism, and crimes against children.

2. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Special Agent, I investigate violent crime against children in violation of 18 U.S.C. §§ 2251, *et seq* and 2421, *et seq*.

3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with a certain Twitter user IDs that is stored at premises owned, maintained, controlled, or operated by Twitter Inc (Twitter), a social networking company headquartered in San Francisco, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under

18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Twitter to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Twitter Username: @JIMMY43845156 at https://twitter.com/jimmy43845156 (**SUBJECT ACCOUNT 1**) and Twitter Username: Alwayshorny695 at https://twitter.com/alwayshorny695 (**SUBJECT ACCOUNT 2**).

5. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of the **SUBJECT ACCOUNT 1 and SUBJECT ACCOUNT 2**.

6. **SUBJECT ACCOUNT 1 and SUBJECT ACCOUNT 2** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252 and 2252A – distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entire content of the **SUBJECT ACCOUNT 1** and **SUBJECT ACCOUNT 2**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

7. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

8. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any

means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

9. As it used in 18 U.S.C. §§ 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) (A) as: actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

10. As it is used in 18 U.S.C. § 2252A, the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

11. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."

12. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

13. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.

[1] The term child pornography is used throughout this affidavit. All references to this term in this affidavit, and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

14. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

IV. BACKGROUND REGARDING THE INTERNET, MOBILE APPLICATIONS AND TWITTER

15. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and conversations with other officers, I know the following:

16. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol addresses and other information both in computer data format and in written record format.

17. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic

[2] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

18. A "server" is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called "clients."

19. "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user's ISP assigns his computer a unique IP address – and that same number is used by the user every time his computer accesses the Internet. Numerical IP addresses generally have corresponding domain names. For instance, the IP address 149.101.10.40 traces to the corresponding domain name "www.cybercrime.gov." The Domain Name System or DNS is an Internet service that maps domain names. This mapping function is performed by DNS servers located throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

20. "Internet addresses" take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can be traced to an identifiable physical location and a computer connection. The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.187). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address, it enables Internet sites to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs. There are two types of IP addresses, dynamic and static. To assign dynamic IP addresses, the ISP randomly assigns one of the available IP addresses, in the range of IP addresses controlled by the ISP, each time a customer dials in or connects to the ISP in order to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot

be assigned to another user during that period. Once the user disconnects, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's dynamic IP address may, and almost always will, differ each time he dials into or connects to the ISP. To assign static IP addresses, the ISP assigns the customer a permanent IP address. The customer's computer would then be configured with this IP address every time he dials in or connects to the ISP in order to connect to the Internet.

21. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

22. Computers connected to the Internet are identified by addresses. Internet addresses take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can identify a physical location and a computer connection.

23. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include LiveMe, KIK messenger service, Snapchat, Meet24, and Twitter.

24. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at http://www.twitter.com. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read 140-character messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

25. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

26. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail

addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

27. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

28. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

29. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's own Tweets, as well as a list of all Tweets that include the user's username (*i.e.*, a list of all "mentions" and "replies" for that username).

30. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

31. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location" function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

32. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with http://t.co. This link service measures how many times a link has been clicked.

33. A Twitter user can "follow" other Twitter users, which means subscribing to those

users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user's "followers" list) and a list of people whom that user follows (*i.e.*, the user's "following" list). Twitters users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

34. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

35. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

36. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

37. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

38. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

39. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user

for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

40. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, communications, "tweets" (status updates) and "tweeted" photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to "tweeted" communications. This geographic and timeline information may tend to either inculpate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner's state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

41. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

V. INVESTIGATION AND PROBABLE CAUSE

42. On or about July 26, 2019, law enforcement officers in Putnam County, New York initiated an investigation into the online sexual exploitation of 14-year-old Minor Victim. Through their investigation, law enforcement identified an individual who both requested and received child sexual abuse materials from Minor Victim via the Kik mobile application. Specifically, that individual communicated with Minor Victim while utilizing the Kik username jimmy.merry04. Law enforcement in New York were able to ascertain that the Kik account associated with the username jimmy.merry04 was registered to James MERRY with a possible address in Muskingum County, OH. The communications between Kik username jimmy.merry04 and the Minor Victim's Kik account began on or about June 27, 2019 and continued until on or about November 24, 2019.

43. On or about January 20, 2020, the Federal Bureau of Investigation (FBI) opened an investigation into the exploitation of Minor Victim by MERRY. In October 2020, the case was then referred to the Muskingum County Sheriff's Office (MCSO) in Zainesville, Ohio and your affiant after it was confirmed that MERRY resided in Ohio within your affiant's jurisdiction. Your affiant then conducted a joint investigation with law enforcement from the MCSO.

44. On or about March 11, 2021, an administrative subpoena was served on Kik requesting subscriber information for Kik username jimmy.merry04. On March 19, 2021, Kik responded to that subpoena with the following information:

Email Address: jimmy.merry23@yahoo.com

Registration Date: December 23, 2014

45. In addition, Kik provided a list of IP addresses that were used to access the Kik account for jimmy.merry04. A subsequent review of the IP address log provided indicated that the following IP addresses were used to access the jimmy.merry04 Kik account at or about the same times the Minor Victim was in contact with the jimmy.merry04 Kik account:

1. 71.72.69.91;
2. 174.233.163.222;
3. 174.233.147.52;
4. 174.233.155.204;
5. 174.233.143.21;
6. 174.233.142.115;
7. 174.233.7.238;

8. 174.233.138.13;
9. 174.233.134.187;
10. 107.11.90.86;
11. 107.11.69.249;

46. Further investigation revealed that eight of the eleven IP addresses from the above noted list were resolved to Verizon Wireless:

1. 174.233.163.222
2. 174.233.147.52
3. 174.233.155.204
4. 174.233.143.21
5. 174.233.142.115
6. 174.233.7.238
7. 174.233.138.13
8. 174.233.134.187

47. Your affiant then learned that three IP addresses provided by Kik were resolved to Charter Communication, specifically, the IP address 71.72.69.91, 107.11.90.86, and 107.11.69.249.

48. On May 18, 2021, an administrative subpoena was served on Charter Communications requesting subscriber information for the IP addresses 71.72.69.91, 107.11.90.86, and 107.11.69.249. On May 21, 2021, Charter Communication responded with the following information regarding IP address 71.72.69.91:

Name: James Merry
Service/Billing Address: 91 N Pembroke Avenue, Zanesville, Ohio 43701
Billing Email: jmerry71@gmail.com
Telephone Number: (740) 453-0633

Charter Communication additionally provided the following information regarding IP addresses 107.11.90.86 and 107.11.69.249:

Name: Douglas Merry
Service/Billing Address: 93731 Ridgeland Dr. Nashport, Ohio 43830
Billing Email: niteowlcop@gmail.com
Telephone Number: (740) 453-0633

49. Your affiant then learned through his investigation that Douglas Merry is the father of James MERRY, the target of the investigation related to Minor Victim.

50. On May 18, 2021, an administrative subpoena was served on Verizon Wireless requesting subscriber information related to the eight IP addresses noted in the Kik subpoena return subscribed to Verizon. On May 19, 2021, in response to an administrative subpoena, Verizon Wireless informed the FBI they only stored IP address records for 365 days. As such they were unable to comply with the subpoena since the information was no longer retained in their database.

51. Based on the registration email listed in the Kik responses, an administrative subpoena was sent to Oath Holdings on April 22, 2021, for subscriber information pertaining to the Yahoo email account jimmy.merry23@yahoo.com. On or about April 28, 2021, in response to an administrative subpoena, Oath Holdings provided the following information:

Name: Jimmy Merry

Subscriber Phone Number: (740) 624-9575

52. Your affiant noted that the telephone number (740) 624-9575 was serviced by Verizon Wireless and an administrative subpoena was then sent to Verizon Wireless to ascertain subscriber information associated with that telephone number. On or about May 13, 2021, in response to the administrative subpoena, Verizon Wireless provided the following information:

Subscriber Name: Douglas Merry

Service/Billing Address: 93731 Ridgeland Dr. Nashport, OH 43830

Identified User: James Merry

Phone Identifiers: Motorola Moto Z2.

53. On or about June 15, 2021, an interview was attempted with James MERRY at the address of 93731 Ridgeland Drive in Nashport, Ohio. Your affiant learned that MERRY was not at the residence but was currently employed at a McDonalds located on the south side of Zanesville, Ohio.

54. On or about June 15, 2021, an interview with MERRY took place at the McDonalds MERRY was employed at. More specifically, MERRY was interviewed in your affiant's FBI vehicle in the McDonalds parking lot. MERRY was advised that his participation in the interview was voluntary and he could leave at any time.

55. During the interview, MERRY admitted to requesting sexually explicit images from Minor Victim as well as other minor children on various social media platforms. MERRY

identified Twitter as one such social media application he utilized to make these requests for child exploitation material. MERRY also admitted to currently possessing sexually explicit images of minor children on his cellular phone, a black Motorola Moto Z2.

56. MERRY signed a written consent for a search of his black Motorola Moto Z2 and provided the cell phone to law enforcement. Your affiant conducted an on-scene review of MERRY's Motorola Moto Z2 and observed what appeared to be sexually explicit images of children. When confronted with this information, MERRY voluntarily surrendered his cellular phone to law enforcement and verbally consented to a forensic examination of his cellular telephone.

57. On or about June 17, 2021, MERRY was arrested by the Muskingum County Sheriff's Office (MCSO) and charged with twelve counts of pandering obscenity involving a minor. On or about August 9, 2021, MERRY plead guilty to those charges and his sentencing hearing is pending.

58. In assisting the MCSO with their investigation of MERRY, the Federal Bureau of Investigations (FBI) took custody of the black Motorola Moto Z2 belonging to MERRY. On July 21, 2021, the FBI completed a forensic analysis of MERRY's black Motorola Moto Z2 cellular telephone.

59. On or about June 22, 2021, the results from the forensic extraction of MERRY's cellular phone were reviewed. Your affiant noted MERRY was in possession of over 75 sexually explicit images of children. In general, these images depicted prepubescent females engaged in the lascivious display of genitalia, masturbation, and sex acts with adults. Specifically, the following sample of child exploitation images were recovered from MERRY's black Motorola Moto Z2:

1. One image depicting a naked prepubescent female, white reclining on a blue sheet with her arms behind her head. The female's legs are bent and spread in such a way as to display her nude genitalia.

2. One image depicting a prepubescent female wearing a pink shirt reclining on a bed with her arms wrapped under her legs, spreading them in such a way as to display her nude genitalia.

3. One image depicting a prepubescent female, white with blond hair wearing a grey t-shirt inserting her fingers into her vagina.

4. One image depicting a prepubescent female wearing a white shirt engaged in

vaginal sex with a male white of undetermined age.

5. One image depicting a prepubescent female bent over displaying her nude genitalia and anus. The minor female is observed to be inserting her fingers into her anus.

6. One image depicting a prepubescent female wearing a pink shirt kneeling on a bed preforming oral sex on the penis of an adult male.

7. One image depicting a prepubescent female wearing pink and white striped underwear engaged in vaginal sex with a male of undetermined age.

60. In reviewing the forensic extraction of MERRY's Motorola Moto Z2, your affiant noted that no Twitter content, including tweets, direct messages, and images were captured during the forensic examination despite the fact that the Twitter application was installed on MERRY's cellular phone.

61. On or about June 23, 2021, your affiant conducted a manual review of the Twitter application that was installed on MERRY's Motorola Moto Z2 cellular phone. Your affiant observed that the Twitter application had a user by the name of @Jimmy43845156, **SUBJECT ACCOUNT 1**, logged in.

62. During the manual review of **SUBJECT ACCOUNT 1** belonging to MERRY, your affiant noted the following exchange of messages occurring between **SUBJECT ACCOUNT 1** and another Twitter user with the Twitter name @AlwaysHorny695, **SUBJECT ACCOUNT 2.** The exchange of messages between both **SUBJECT ACCOUNTS** took place on June 10, 2021. The following is an excerpt from the communications between the two **SUBJECT ACCOUNTS:**

AlwaysHorny695: Got any pics of young teens

Jimmy43845156: Yeah why WBU [What about you]

AlwaysHorny695: Yeah send some?

Jimmy43845156: Clothed or nude

AlwaysHorny695: Nude

MERRY then sent one image to AlwaysHorny695 which your affiant was unable to view on the Motorola Moto Z2. In response to that photo, @AlwaysHorny695 requested "a couple please." MERRY then sent three additional images to @AlwaysHorny695 which your affiant was unable to view on the Motorola Moto Z2. You affiant then noted the following conversation:

AlwaysHorny695: More please I'm close. Need a few more before I cum

Jimmy43845156: You gotta send some first.

You affiant observed that @AlwaysHorny695 then sent four images to MERRY which your affiant was unable to view on the Motorola Moto Z2. After @AlwaysHorny695 sent the messages, he indicated to MERRY that "some of them are my ex's."

63. The conversation between **SUBJECT ACCOUNT 1** and **SUBJECT ACCOUNT 2** continued on June 10, 2021. The following is an additional excerpt from that day between the **SUBJECT ACCOUNTS:**

Jimmy43845156: If you got more young or something else to offer

AlwaysHorny695: Yeah hold on.

Jimmy43845156: Okay

AlwaysHorny695: My ex's okay. They're young.

Jimmy43845156: How old

AlwaysHorny695: 12. 13. 15.

Jimmy43845156: Any of them got a Twitter account or anything

AlwaysHorny695: No mate but I have their nudes

Jimmy43845156: Show

You affiant observed that @AlwaysHorny695 then sent four images to MERRY which your affiant was unable to view on the Motorola Moto Z2. After the first image @AlwaysHorny695 sent a message with the numbers 12. After the second image AlwaysHorny695 sent a message with the numbers 15. After the third image @AlwaysHorny695 sent a message with the numbers 14. After the fourth image AlwaysHorny695 sent a message with the numbers and 16. Based on the nature of the conversation, your affiant believes these numbers from @AlwaysHorny695 following the respective image are indicative of the age of the minor depicted in the image sent to MERRY.

64. Upon receiving the four images above, MERRY stated "that 12yr old can come and make her way over onto y cock now" to which @AlwaysHorny695 responded "Haha and mine she gave amazing blowjobs."

65. On or about 16 June 2021, a preservation letter was served on Twitter for **SUBJECT ACCOUNT 1.**

66. On or about 29 June 2021, a preservation letter was served on Twitter for **SUBJET ACCOUNT 2.**

67. On or about July 8, 2021, in response to the administrative subpoena sent for

subscriber information on **SUBJECT ACCOUNT 1,** Twitter identified the following information for **SUBJECT ACCOUNT 1:**

Telephone Number: (740) 624-9575

68. Your affiant noted that the phone number associated with the **SUBJECT ACCOUNT 1** was the same phone number provided by Oath Holdings in April 2021 which identified Jimmy Merry as the account holder for the Yahoo email account jimmy.merry23@yahoo.com.

VI. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN MINORS.

69. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved receiving, distributing, and/or collecting child pornography:

1. Those who exchange and/or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.
2. Those who trade and/or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
3. Those who trade and/or collect child pornography sometimes maintain hard copies of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some

other secure location. These child pornography collections are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

4. Those who trade and/or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and have been known to maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
5. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

70. Based upon the conversations between MERRY, who was utilizing **SUBJECT ACCOUNT 1** and the unknown individual utilizing **SUBJECT ACCOUNT 2,** and the facts learned during the investigation in this case, namely, that MERRY admitting to requesting and possessing child pornography on Twitter, your affiant has reason to believe that MERRY has a sexual interest in minors and has viewed, sought out, received, or distributed visual depictions of minors engaged in sexually explicit conduct. Your affiant therefore submits that there is probable cause to believe the evidence of the offenses of receipt, distribution, and possession of child pornography will be located on the **SUBJECT ACCOUNTS.**

VII. CONCLUSION

71. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2252 and 2252A have been committed, and evidence of those violations is located on **SUBJECT ACCOUNT 1** and **SUBJECT ACCOUNT 2**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNTS** described in Attachment A, and the seizure of the items described in Attachment B.

Andrew D. McCabe
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this _____ day of August 2021.
August 23, 2021

Kimberly A. Johnson
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Twitter Username: @Jimmy43845156 at https://twitter.com/jimmy43845156 and Twitter Username: Alwayshorny695 at https://twitter.com/alwayshorny695 which are the subject of a preservation request sent to Twitter Inc., on June 16, 2021 and June 29, 2021 respectively, that is stored at premises owned, maintained, controlled, or operated by Twitter Inc., a company headquartered at 1355 Market Street, Suite 900, San Francisco, CA 94103.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

I. Information to be disclosed by Twitter Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment A:

(a) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(b) All past and current usernames, account passwords, and names associated with the account;

(c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(d) All IP logs and other documents showing the IP address, date, and time of each login to the account;

(e) All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

(f) All "Tweets" and Direct Messages sent, received, "favorited," or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;

(g) All information from the "Connect" tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of

all Tweets that include the username associated with the account (*i.e.*, "mentions" or "replies");

(h) All photographs and images in the user gallery for the account;

(i) All location data associated with the account, including all information collected by the "Tweet With Location" service;

(j) All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;

(k) All data and information that has been deleted by the user;

(l) A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user's "following" list and "followers" list);

(m) A list of all users that the account has "unfollowed" or blocked;

(n) All "lists" created by the account;

(o) All information on the "Who to Follow" list for the account;

(p) All privacy and account settings;

(q) All records of Twitter searches performed by the account, including all past searches saved by the account;

(r) All information about connections between the account and third-party websites and applications;

(s) All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. Information to be seized by the government

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252 and 2252A – distribution, transmission, receipt, and/or possession of child pornography:

(a) Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Twitter account owner;

(b) Evidence indicating the Twitter account owner's state of mind as it relates to the crime under investigation; pertaining to the coercion, enticement or intent to travel in interstate commerce to engage in illicit sexual activity.

(c) Evidence of communications related to the distribution, transmission, receipt, and/or possession of child pornography.

(d) Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts.